Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1820 05/20/16

~ Computer Held Hostage! ~ People Are Talking! ~ Changes to Chrome!
~ Falcon King Solitaire! ~ New Police Camouflage! ~ Wi-Fi Sense Gone!
~ El Capitan Is Updated! ~ Hell Is Hot, in Doom! ~ Twitter 140 Tweak!

-* British Hacker Wins A Battle *-
-* Atari Has "Haunted House" Exclusive? *-
-* Google May Get Hit With EU Antitrust Fine! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

It’s starting to feel more and more like Spring, finally! Here we are, nearing Memorial Day, and the temps have been ranging around early Spring numbers rather than late Spring. I guess it’s better late than not at all! It’s also time to head out and pick up a new barbecue grill; the old one is rusting out all over! It’s just plain un-American not to do a little barbecuing over the long holiday weekend!

I’m tempted to talk politics this week, but I’m not going to go in that direction again this week. Nope, not going there!

So, while we all relax and start making preparations for Memorial Day, I’ll just mosey along and get right into this week’s issue!

Until next time...

=~=~=~=

Falcon 030 King Solitaire

Hello!

Cleaning my hard disk....
Playable on Falcon 030, VGA and 4 Mb of ram min.

Download : http://paradize.final-memory.org/games.shtml
Enjoy !

=~=~=~=

->In This Week’s Gaming Section - Hell Is Hot, Multiplayer’s Not in Doom
"""""""""""""""""""""""""""""" Atari Argues Only It Can Make ’Haunted House’

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""""

Hell Is Hot, Multiplayer's Not in Gloriously Gory Doom

It s been 12 years since the release of Doom 3. That s more than a decade without chainsaws and miniguns and super shotguns and BFGs. Without Cyberdemons and Imps and Hell Knights and a solitary space marine with a nasty right hook.

God, I ve missed it.

But it s back. Doom has finally returned, and developer id Software has taken its latest entry in the infamous first-person franchise back to its roots. Hell, even the game s title is a throwback. And it s for the better, because for all its heavy-metal fury, Doom is flat-out fun.

Unlike 2004 s Doom 3, which focused heavily on foreboding atmosphere, jump scares, and the need to use a flashlight to see what was happening 95 percent of the time, the new Doom harkens back to the simple joy of battling wave after wave of demons and exploring hidden rooms the stuff that made the original Doom and its sequel such beloved (and influential) shooters.

Indeed, this is a game out of time. It eschews the excessive narrative exposition or grandiose ruminations on the human condition you ll see in many of today s games. This is a game about cutting monsters in half with a goddamn chainsaw, and it makes no apologies for it.

As usual, you play as a nameless space marine whose goal is to blast armies of demons off of Mars and back to Hell. Why are demons invading Mars? Something, something, power source, something, something. It doesn t matter. Doom lets you know its intentions from the very outset. The game s first scene sees you chained to a sarcophagus, only to break free and smash a demon s skull to bits with your bare hands.

And that s pretty much the gist of Doom s campaign. Through the first hour or so, you traverse nondescript hallways, blasting some easy demons while slipping around in the entrails of the employees of Union Aerospace Corporation, who made the unfortunate decision to solve Earth s energy crisis by opening up a portal to Hell. That obviously didn t work out too well.

Once you reach the Martian surface, the game really opens up. Each time Doom introduces a new type of enemy, you ll think it s some kind of intense boss battle. But after you finally kill your new foe, the game starts throwing them at you by the truckload. That

wasn t a boss battle, that was Doom s way of letting you know that the party s just getting started.

The first time this happened to me, I was battling a Revenant, a demon with giant guns on its shoulders. I pumped my entire payload into it before it fell. After regrouping for a second and moving into the next area, there were three more waiting for me. Doom is a cruel teacher, testing you over and over, and just before you break, it gives you a short breather before it throws even more your way.

Luckily, you re capable of carrying an enormous weapons cache on your broad marine shoulders. Doom adds a good amount of upgrading and customizations to the mix, too. You can, for example, attach a scope to your heavy machine gun to pick off Imps from a distance, or slap on an attachment that fires six rockets in succession.

You earn weapon upgrade points by completing in-game challenges displayed in the pause menu. Unfortunately, the menu is a bit too cluttered and clunky, which makes finding the challenges a, well, challenge. Naturally, you can also upgrade your Praetor Suit to increase your health, armor, or ammo capacity.

And make no mistake you ll need to upgrade everything to keep up with Doom s frenetic pace. This is a blazing fast shooter, and while armor and health pickups initially seem plentiful, they quickly vanish in the game s many large-scale fights.

To make things a little easier, Doom introduces Glory Kills, melee attacks that yield Doom s most brutal moments and, more pleasantly, a cache of health pickups. They re gruesome, disgusting, and all too satisfying. Over time you start to depend on these up-close attacks to stay alive, turning even the most passive player into an aggressive, forward-charging maniac.

Eventually, however, the chaos wears a little thin. After fighting wave after wave of demons, battles start to blend together, making each fight feel less remarkable than the last. Doom always throws a new challenge at you before the game begins to feel rote, but the campaign s later stages just aren t as thrilling as they should be.

Doom is technically impressive as well, buttery smooth with nary a framerate hiccup. That said, the PlayStation 4 version of the game, which I reviewed, doesn t offer nearly the graphical punch as the PC version. Textures occasionally pop in, and the outdoor scenery looks particularly bland. I get that I m supposed to be looking at a desolate Martian landscape, but do the boulders have to look like blobs of orange Jell-O?

Doom also features a full-fledged multiplayer component, though it sadly can t match the solo experience. You get six gameplay modes, including standard Team Deathmatch and Domination as well as offerings like Soul Harvest, which sees you collect the souls of your opponents for points. There are plenty of opportunities for character customization and upgrades, but the whole experience suffers from some particularly uninspired levels.

It s partly by design Doom embraces its old-school sensibilities everywhere - but compared to the exciting, dynamic levels in games like Call of Duty Black Ops 3 and Overwatch, Doom s multiplayer

just doesn t hold up. Sure, if you re playing with a group of friends, you ll still have a good time with Doom, but you ll likely find yourself tiring of it rather quickly.

There is hope for Doom s multiplayer, though, in the form of SnapMap. A built-in multiplayer level editor, SnapMap lets you design your own hellish playground in which you and your friends can hunt demons and generally cause a ruckus. It s called SnapMap because you literally snap chunks of the world together like giant blood-drenched puzzle pieces.

It s not just about slapping levels together, though. You can also add demons, in-game effects, weapon drops, anything you can see in the single-player campaign. It s incredibly intuitive you can put together a level in a few minutes and start playing right away.

So kudos to id and Bethesda for managing to make an old game feel new again. That s not easy to do, and while its multiplayer stumbles, Doom will leave you exhausted from its intensity, sick from its brutality, and yearning for more when you complete its 13-hour campaign. If you like your shooters fast and deadly, Hell is pretty heavenly.

What s hot: Ridiculously fast-paced combat; satisfying weapons upgrades; Glory Kills; CHAINSAWS!

What s not: Mediocre multiplayer; occasionally bland graphics; battles can blend together

Platform reviewed: PS4

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Ex-Game Maker Atari To Argue To The US PTO That Only It Can Make ’Haunted House’ Games

We noted several years ago that Atari, once the king of the video game industry, has since devolved into a zombie company built only for intellectual property trolling. Copyright, trademark, or patents: Atari will use all of them to try to milk the modern gaming industry for cash. In fact, in past public statements, Atari has made it clear that it has no interest in producing any new games, instead relying on its remaining staff to license its trademarks and port a few decades-old games over to the mobile market. Quite a fall for the once giant of the industry.

And that fall will now include going in front of the PTO’s Appeal Board to explain why Atari and Atari alone should be allowed to title a game using the phrase "Haunted House." Why? Well, because

it made a game called Haunted House in the early 80’s, you see.

The United States Patent and Trademark Office has set oral arguments for Atari s claim against developer Hazy Dreams of Infinity over its use of Haunted House in the game Haunted House Tycoon. Atari and defendant Andrew Greenberg, Hazy Dreams founder, present oral arguments on Thursday. In 2011, Atari filed a notice of opposition against the Hazy Dreams in an effort to prevent the developer from launching the game, which is still in development. The classic-gaming publisher s stance is that it owns that trademark in the gaming industry after releasing Haunted House in 1982 for the Atari 2600 console although Atari did not file for that mark until 2010.

So Atari is going to bully a current game maker over a generic term it once used on a game it made over three decades ago, but didn’t trademark until 2010. It’s hard to think of an example that better shows how trademark law is abused today, deviating from its intended purpose and spirit. There’s no customer confusion here to worry about. Nobody is going to mistake Atari’s block graphics for the modern Haunted House Tycoon title. This is simply a bullying tactic, likely to generate licensing revenue. That’s what Atari is now, after all.

Greenberg, of course, isn’t pleased.

Trying to claim no one else can use the words Haunted and House is especially ridiculous, considering games have been using the term Haunted House in titles ever since Magnavox released a game by that name for the Odyssey in 1972, he said in a statement. Atari has a horrible reputation for attacking independent game developers, including recently going after TxK developer Jeff Minter, the Hazy Dreams of Infinity president said.

That’s true, of course, but the folks running Atari these days don’t care about that reputation. It isn’t the public that is making them money, after all.

All of this comes as Atari has lost much of its original identity. The company, which has shifted from owner to owner over time, filed for bankruptcy in 2013. It emerged later that year under the ownership of venture capitalist Frederic Chesnais, who says that company is now 10 people primarily responsible for managing its past assets.

Ten people working for a company designed to troll actual makers of gaming content, potentially successfully blocking the release of a game because it carries a fairly generic phrase in its title? Yeah, we’ve gotten so far away from the original purpose of trademark at this point that it’s basically unrecognizable.

=~=~=~=

Compiled by: Dana P. Jacobson

Google May Get Hit With Record EU Antitrust Fine

Google may face a record antitrust fine from the European Commission in the coming weeks, according to the British newspaper The Sunday Telegraph.

The EU is considering levying a fine of about 3 billion euros ($3.4 billion) against the web giant over its dominance in the search market, the newspaper reported. Google did not immediately respond to a request for comment.

Google and the European Union have engaged in a drawn-out battle over search for six years. At issue are the EU's claims that Google has abused its position as the world's most dominant search engine in unfairly prioritizing its shopping services over those of competitors.

The EU's probe of Google began in 2010 but has repeatedly stalled because the company and the commission could not agree on settlement terms.

The biggest antitrust fine to date was the 1.06 billion euros ($1.45 billion) levied against Intel in 2009 for engaging in illegal anticompetitive practices to exclude competitors from the market for computer chips.

British Hacker Wins Legal Battle Over Encryption Keys

Britain's top crime fighting force has failed in a legal attempt to force alleged hacker Lauri Love to hand over his hard disk's encryption keys. In a landmark case, District Judge Nina Tempia said the investigative agency should have used the normal police powers rather than a civil action to obtain the evidence. Lauri Love, a 31-year-old hacker, has been accused of aiding cyber-attacks against U.S. targets, including NASA, FBI, US Army and US Federal Reserve networks.

The National Crime Agency (NCA) has failed in a legal attempt to force the British citizen and political hacktivist Lauri Love to hand over the keys to encrypted data that has been seized from his home two years ago.

At a Tuesday hearing in Court Seven at Westminster Magistrates' Court, the NCA's application to make Love disclose his encrypted computer passwords was refused by the judge.

Love, 31, is currently fighting extradition to the United States where he faces up to 100 years in prison for allegedly hacking into the Federal Bureau Investigation (FBI), the National Aeronautics and Space Administration (NASA), the US Missile Defence Agency, and Federal Reserve Bank of New York during 2012 and 2013.

United States Prosecutors claim that Love was allegedly involved in the online protest #OpLastResort linked with the Anonymous group, following the untimely death of online activist Aaron Swartz, who committed suicide in 2013 while under federal charges of data theft.

Love was initially arrested from his home in Stradishall, England back in October 2013, when the British police seized his encrypted computers and hard drives. The NCA later asked the courts to force Love to turn over keys to decrypt his computer's hard drives.

The files that authorities say could contain data from the US Senate and the Department of Energy on Love's computer has been encrypted with Truecrypt, a popular software for encrypting data.

Initially, the British agency attempted to compel Love to hand over his encryption keys and passwords under Section 49 of the Regulation of Investigatory Powers Act (RIPA) 2000, but was failed after his refusal.

Love, who is currently on bail, launched a legal action against the NCA to return his computer equipment. However, the agency refused, claiming the devices could contain data that he did not legally belongs to him for example, hacked files.

So, as part of those civil proceedings, the agency made an application to force Love to hand over his "encryption key or password" for the encrypted data found on his computer and hard drives.

However, Judge Nina Tempia of Westminster Magistrates' Court in London ruled in favor of Love, saying the NCA can not force Love to disclose his passwords and encryption keys to prove his ownership of the data.

Tempia also said the NCA has attempted to "circumvent" the RIPA act, which she described as the "specific legislation that has been passed to deal with the disclosure sought."

"I am not granting the application because to obtain the information sought the correct procedure to be used, as the NCA did two-and-a-half years ago, is under section 49 RIPA, with the inherent HRA safeguards incorporated therein," Tempia wrote in her ruling on Tuesday.

The NCA has yet to comment on the court proceedings. However, Love was "happy" with the result. Speaking outside court, he said: "It is a victory, although it is a more an avoidance of disaster."

The court hearing revolving around the return of Love's computer equipment is scheduled for July 28.

Police Camouflage Surveillance Truck as Google Maps Van

I bring good news.

If you live in Philadelphia and you're concerned that Google's Street View vans are spying on you, relax.

It might merely be your friendly local police instead.

I deduce this after Matt Blaze, a University of Pennsylvania assistant professor of computer and information science, tweeted a photograph of a van that had a Pennsylvania Police Department placard and a Google Maps logo on its window.

As Motherboard reports, he espied it near the Philadelphia Convention Center. It was equipped with two sophisticated license-plate readers on its roof.

Why, though, would the police wish to pretend - and so obviously - that one of its surveillance vehicles was actually just mapping the roads for Google?

Neither the Philadelphia Police Department nor Google responded to requests for comment.

But the police department did issue this statement to Motherboard: "We have been informed that this unmarked vehicle belongs to the police department. However, the placing of any particular decal on the vehicle was not approved through any chain of command. With that being said, once this was brought to our attention, it was ordered that the decals be removed immediately."

The department added that it is investigating what might have happened.

Police spokesman Lt. John Stanford told NBC Philadelphia that his officers were "being creative." Is that as in "creative with the truth"?

What of Google, though? One might imagine it would be outraged that its auspices had been co-opted by the police. The ELSAG MPH-900 equipment mounted on the truck is highly efficient and can capture many license plates simultaneously. That's not the sort of thing Google would wish to be involved in, surely.

There again, we're all being surveilled multiple times by multiple organizations. Some police forces have reportedly used Stingray devices, which pretend to be cell towers but actually monitor all calls within the vicinity, without a warrant.

And Google, Facebook and the rest follow us around the Web like men in beige coats and shades, wanting to know about our likes and behaviors.

We're trapped.

How odd, though, that a police force would want to pretend that we're trapped by Google rather than the authorities. Doesn't that show a slight lack of self-worth?

What To Do If Hackers Hold Your Computer Hostage and Demand Cash

You re sitting at your computer when you get an email from your local bank saying you were just hit with a charge for a new $1,200 MacBook that you never bought. You click the email and follow the embedded link or download the included receipt to find out what s up.

Just like that, your computer has been infected with ransomware. You can t access your files, and all you can see is a timer counting down the time until hackers delete your computer s drive unless you pay them a fee in iTunes gift cards.

All you can do is scratch your head and wonder what the hell just happened. Well, I m here to explain that to you and to help you fight back against ransomware criminals.

The most important thing to remember is this: Never, ever pay the ransom.
Ransom?

Let s start with the basics. A particularly nefarious form of malware, ransomware is a piece of software criminals use to lock you out of your computer by encrypting its files and holding them for ransom for a specific dollar amount.

If you don t pay up, you can potentially say goodbye to your photos, tax documents, pay stubs, and any other documents you ve saved throughout the years.

This isn t some idle threat, either. If you don t pay, your documents will disappear or simply stay locked up until you completely reformat your system.

Ransomware programs sometimes require you to pay in Bitcoin, an anonymous currency that can t be tracked.

However, criminals have increasingly begun demanding payment in the form of iTunes or Amazon gift cards, since the average person doesn t know how to use Bitcoin, according to Gary Davis, chief consumer security evangelist at Intel Security.

The amount you have to pay to unlock your computer can vary, with some experts saying criminals will ask for up to $500.

To be clear, ransomware doesn t just target Windows PCs. The malware has been known to impact systems ranging from Android phones and tablets to Linux-based computers and Macs.

According to Davis, ransomware was actually popular among cybercriminals over a decade ago. But it was far easier to catch the perpetrators back then since anonymous currency like Bitcoin didn t exist yet. Bitcoin helped changed all that by making it nearly impossible to track criminals based on how victims pay them.

There are multiple types of ransomware out there, according to Chester Wisniewski, a senior security advisor with the computer security company Sophos. Each variation is tied to seven or eight criminal organizations.

Those groups build the software and then sell it on the black market, where other criminals purchase it and then begin using it for their own gains.

How they get you

Ransomware doesn t just pop up on your computer by magic. You actually have to download it. And while you could swear up and down that you d never be tricked into downloading malware, cybercriminals get plenty of people to do just that.

For example, hackers can determine your location and send emails that look like they re from companies based in your country.

Criminals are looking are looking up information about where you live, so you ll click (emails), Wisniewski explained to Yahoo Finance. So if you re in America, you ll see something from Citi Bank, rather than Deutsche Bank, which is in Germany.

Cybercriminals can also target ransomware messages to the time of year. So if it s the holiday shopping season, criminals might send out messages supposedly from companies like the US Postal Service, FedEx or DHL. If it s tax time, you could receive a message that says it s from the IRS.

Other ransomware messages might claim the FBI has targeted you for using illegal software or viewing child pornography on your computer. Then, the message will tell you to click a link to a site to pay a fine only to lock up your computer after you click.

It s not just email, though. An attack known as a drive-by can get you if you simply visit certain websites. That s because criminals have the ability to inject their malware into ads or links on poorly secured sites. When you go to such a site, you ll download the ransomware. Just like that, you re locked out of your computer.

Ransomware attacks vulnerabilities in outdated versions of software. So, believe it or not, the best way to protect yourself is to constantly update your operating system s software and apps like Adobe Reader. That means you should always click that little update notification on your desktop, phone, or tablet. Don t put it off.

Beyond that, you should always remember to back up your files. You can either do that by backing them up to a cloud service like Amazon Cloud, Google Drive or iCloud, or by backing up to an external drive.

That said, you ll want to be careful with how you back up your content. That s because, according to Kaspersky Lab s Ryan Naraine, some ransomware can infect your backups.

Naraine warns against staying logged into your cloud service all the time, as some forms of malware can lock you out of even them. What s more, if you re backing up to an external hard drive, you ll want to disconnect it from your PC when you re finished, or the ransomware could lock that, as well.

Naraine also says you should disconnect your computer from the internet if you see your system being actively encrypted. Doing so, he explains, could prevent all of your files that have yet to be encrypted from being locked.

Above all, every expert I spoke with recommended installing some form of anti-virus software and some kind of web browser filtering. With both types of software installed, your system up to date, and a backup available, you should be well-protected.

Oh, and for the love of god, avoid downloading any suspicious files or visiting sketchy websites.

Even if you follow all of the above steps, ransomware could still infect your computer or mobile device. If that s the case, you have only a few options.

The first and easiest choice is to delete your computer or mobile device and reinstall your operating system. You ll lose everything, but you won t have to pay some criminal who s holding your files hostage.

Some security software makers also sell programs that can decrypt your files. That said, by purchasing one, you re betting that it will work on the ransomware on your computer, which isn t always the case. On top of that, ransomware makers can update their malware to beat security software makers offerings.

All of the experts agree that the average person should never pay the ransom even if it means losing their files. Doing so, they say, helps perpetuate a criminal act and emboldens ransomware makers.

Even if you do pay up, the ransomware could have left some other form of malware on your computer that you might not see.

In other words: Tell the criminals to take a hike.

Google Is Making A Major Change To Chrome To Make The Internet More Secure

As long as there s been a modern Internet, there s been Adobe Flash. And as long as there has been Adobe Flash, there have been webmaster and internet nerds who loathe it with every fiber of their being. So they re celebrating that by the end of the year, Flash will effectively be banned from Google Chrome. But why is Google doing this, and what does it mean for you?

Adobe Flash is, at root, an animation program; back in the mid 90s, it was created to build vector graphics and cartoons for web applications. Over time, it became more complex and feature-rich, allowing users to build programs inside Flash. These started as simple web games but have become more and more elaborate over time.

Unfortunately, it s also meant that Flash is, by far, the easiest way for hackers to breach your computer and execute malicious

code. In fact, Flash is probably the biggest security problem on the internet and it s been criticized as such for nearly 20 years. The iPhone doesn t allow Flash for precisely this reason. Facebook wants to phase it out entirely and older versions of the Flash player aren t allowed to interact with modern browsers. The internet s common language, HTML, was updated with a host of new features specifically designed to get rid of Flash.

It s a credit to how persistent Flash is that Chrome can t kill it entirely. But what it is doing is, aside from a handful of major websites, blocking Flash by default, although it will prompt you to enable Flash if you trust the site in question. That would seem a near-fatal blow, forcing websites to either update to HTML 5 or risk being functionally invisible to much of the Internet. Then again, Flash has outlived two different companies that have owned it and survived Apple rejecting it, so it s hard to believe this might be the final straw

On a practical level, not much will likely change for your average internet user, aside from the fact that restaurants will finally update their websites. It will mean you run into a lot fewer security problems on Chrome. But since the future is full of fascinating new ways hackers can make your life miserable, you ll likely be too preoccupied to notice.

Microsoft Removes Its Controversial Windows 10 Wi-Fi Sense Password Sharing Feature

Microsoft has finally decided to remove one of its controversial features Wi-Fi Sense network sharing feature from Windows 10 that shares your WiFi password with your Facebook, Skype and Outlook friends and enabled by default.

With the launch of Windows 10 last year, Microsoft introduced Wi-Fi Sense network sharing feature aimed at making it easy to share your password-protected WiFi network with your contacts within range, eliminating the hassle of manually logging in when they visit.

This WiFi password-sharing option immediately stirred up concerns from Windows 10 users especially those who thought the feature automatically shared your WiFi network with all your contacts who wanted access.

But Wi-Fi Sense actually hands over its users controls so they can select which networks to share and which contact list can access their Wi-Fi.

Also, the feature doesn’t share the actual password used to protect your Wi-Fi, but it does give your contacts access to your network.

However, the biggest threat comes in when you choose to share your Wi-Fi access with any of your contact lists.

But, Who really wants to share their Wi-Fi codes with everyone in the contacts?

Of course, nobody wants.

Since the feature doesn't give you the option to share your network with selected individuals on Facebook, Skype or Outlook, anyone in your contact list with a malicious mind can perform Man-in-the-Middle (MITM) attacks.

We have written a detailed article on Wi-Fi Sense, so you can read the article to know its actual security threat to Windows 10 users.

Although Microsoft defended Wi-Fi Sense network-sharing as a useful feature, Windows users did not give it a good response, making the company remove WiFi Sense's contact sharing feature in its latest Windows 10 build 14342.

"The cost of updating the code to keep this feature working combined with low usage and low demand made this not worth further investment," said Microsoft Vice President Gabe Aul. "Wi-Fi Sense, if enabled, will continue to get you connected to open Wi-Fi hotspots that it knows about through crowdsourcing."

Microsoft just released its latest Windows 10 build for testers. The company will remove the Wi-Fi Sense password sharing feature as part of its Anniversary Update due in the summer, but will keep the Wi-Fi Sense feature that lets its users connect to open networks.

Apple Releases OS X 10.11.5 El Capitan With Bug Fixes and Performance Improvements

Apple recently released OS X 10.11.5 to the public, marking the launch of the fifth update to the El Capitan operating system that was first released on September 30, 2015. OS X 10.11.5 comes nearly two months after the release of OS X 10.11.4, an update that introduced Live Photos for Messages and password protected notes in the Notes app.

The OS X 10.11.5 update can be downloaded through the Software Update mechanism in the Mac App Store. It is available to all OS X El Capitan users.

Most of the updates to OS X El Capitan have focused largely on under-the-hood improvements, bug fixes, and security enhancements rather than outward-facing changes, and OS X 10.11.5 is no exception. No obvious feature changes were discovered in the beta, and according to Apple's release notes, OS X 10.11.5 includes bug fixes, performance improvements, and security updates.

Prior to releasing the OS X 10.11.5 update, which has been in testing since April 6, Apple seeded four betas to developers and public beta testers.

Twitter To Stop Counting Photos and Links in 140-Character Limit

Twitter Inc. is making a major shift in how it counts characters in Tweets, giving users more freedom to compose longer messages.

The social media company will soon stop counting photos and links as part of its 140-character limit for messages, according to a person familiar with the matter. The change could happen in the next two weeks, said the person who asked not to be named because the decision isn t yet public. Links currently take up 23 characters, even after Twitter automatically shortens them. The company declined to comment.

It s a step in a larger plan to give users more flexibility on the site. Chief Executive Officer Jack Dorsey said in January that the company was looking for new ways to display text on Twitter, and would experiment based on how people use the service. For example, some people tweet screenshots of longer text in articles, or send many tweets one after the other to tell a story.

Twitter s 140-character limit was originally adopted because it was a way to send Tweets while fitting all the information within a mobile text message -- a common way for sending Tweets when the service debuted in 2006, before the proliferation of smartphones.

The company earlier this year considered raising the limit to as many as 10,000 characters. But the quick, concise nature of Tweets has helped set the site apart from the competition. Executives have spent the last few months emphasizing how Twitter is a destination for live events and discussion. Removing the character requirement for links and photos may encourage users to add more media to their posts.

Twitter has been making video a priority as part of its push for live events. Earlier this year, the company agreed to pay $10 million to the National Football League for the rights to stream 10 Thursday night games during the 2016 season, people familiar with the matter have said. Twitter is working on more content deals for streaming sports, political events and entertainment.

=~=~=~=

Atari Online News, Etc.